НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання лабораторної роботи

ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ ЗАХИЩЕНИХ МЕСЕНЖЕРІВ ТИПУ SKYPE, VIBER, WHATSAPP, SIGNAL

Виконали студентки
групи ФІ-32мн
Зацаренко А. Ю.
Футурська О.В.

Київ — 2024

ЗВІТ

1.1 Мета комп'ютерного практикуму

Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP.

1.2 Постановка задачі

Проаналізувати існуючу інформацію про системи Viber, WhatsApp, Skype, Telegram та їх криптографічні механізми. Детально розібрати опис усіх механізмів протоколу, структуру пакетів та характеристики систем. Довести теоретично можливість існування в системі виявлених протоколів та зробити огляд відомих аналізів захищеності вказаних протоколів, включаючи вже виправлені помилки. Зробити порівняльний аналіз можливостей вказаних систем, їх криптографічних механізмів та рівня захищеності (обґрунтований). Дати рекомендації користувачам щодо безпечного використання таких систем.

1.3 Хід роботи

У сучасному світі захист інформації є одним із ключових аспектів цифрової комунікації. Месенджери, такі як Skype, Telegram, WhatsApp та Viber, широко використовуються для особистого та професійного спілкування, забезпечуючи користувачам зручність і швидкість передачі даних. Однак безпека цих систем викликає чимало питань, оскільки приватність спілкування залежить від криптографічних механізмів, які вони використовують. У цьому дослідженні ми проведемо детальний аналіз особливостей кожної з цих платформ, їх протоколів, рівня захищеності та надамо рекомендації щодо їх безпечного використання.

1.3.1 Аналіз існуючої інформації про Skype та його криптографічні механізми

Skype — це популярний додаток для обміну повідомленнями, аудіо- та відеодзвінків, який належить корпорації Microsoft. Система використовує різні криптографічні механізми для забезпечення безпеки комунікацій. Основними аспектами криптографії у Skype є:

• Аутентифікація користувачів. У Skype використовуються облікові записи Microsoft, для яких аутентифікація забезпечується протоколом OAuth 2.0 та шифруванням SSL/TLS під час передавання даних.

• Шифрування даних. Для забезпечення конфіденційності застосовуються алгоритми AES (Advanced Encryption Standard) із 256-бітним ключем.

• Передача ключів. Skype використовує асиметричну криптографію для обміну ключами, зокрема алгоритм RSA.

• End-to-end шифрування. Skype підтримує захист особистих чатів за допомогою протоколу Signal, який гарантує, що повідомлення доступні лише відправнику та отримувачу.

1.3.2 Опис механізмів протоколу, структури пакетів та характеристик системи Skype

Skype базується на пропрієтарному протоколі **Skype Protocol**, що використовує поєднання однорангової (peer-to-peer) архітектури та серверної підтримки для маршрутизації даних. Основні етапи роботи протоколу:

1) Ініціалізація з'єднання:

* Користувач проходить аутентифікацію через сервери Microsoft.

* Після успішної аутентифікації встановлюється з'єднання з іншими учасниками через P2P-мережу або сервери.

2) Передача даних:

* Повідомлення та медіадані шифруються за допомогою AES і передаються через UDP або TCP в залежності від типу з'єднання.

* Використовується додаткове SSL/TLS шифрування для безпечного транспортування даних через інтернет.

3) Структура пакетів:

* Пакети Skype містять заголовок із метаданими (ідентифікація сесії, тип повідомлення тощо) та зашифрований корисний вміст.

* Заголовки забезпечують маршрутизацію даних у P2P-мережі або через сервери.

Характеристики системи:

– Швидкість роботи. Skype оптимізує маршрути передачі даних через P2P-мережу для зменшення затримок.

– Надійність. Завдяки поєднанню серверів і одноранговоі архітектури забезпечується стабільність зв'язку навіть при низькій якості інтернету.

– Мобільність. Skype доступний на різних платформах, включаючи Windows, macOS, iOS, Android.

1.3.3 Теоретичне обґрунтування можливих вразливостей протоколу Skype

Незважаючи на потужні криптографічні механізми, Skype має потенційні вразливості, які аналізувалися дослідниками:

1) Закритий характер протоколу. Через те, що протокол Skype є пропрієтарним, дослідження його безпеки обмежені. Це ускладнює виявлення прихованих недоліків.

2) Зловживання в одноранговій мережі. Атаки типу man-in-the-middle (MitM) можуть бути виконані в мережах з недостатнім захистом, якщо зловмисник контролює один із вузлів.

3) Уразливість кінцевих точок. End-to-end шифрування впроваджене лише для особистих чатів. Інші типи комунікацій можуть бути менш захищеними.

4) Історичні проблеми. У минулому були виявлені вразливості, наприклад, в способі генерування криптографічних ключів, які згодом виправлені.

Відомі дослідження:

– Дослідники неодноразово піддавали критиці протокол Skype за відсутність прозорості.

– Відомо, що у 2013 році Skype співпрацював із державними органами для доступу до метаданих, що викликало сумніви щодо його конфіденційності.

Таким чином, хоча Skype використовує сучасні криптографічні механізми, закритість протоколу і вразливість кінцевих точок залишають простір для покращення захищеності системи.

1.3.4 Аналіз існуючої інформації про Telegram та його криптографічні механізми

Telegram — це месенджер, створений із фокусом на швидкість, безпеку та простоту використання. Для забезпечення конфіденційності даних Telegram використовує власний протокол **MTProto**. Основними криптографічними механізмами Telegram є:

• Аутентифікація користувачів. Telegram використовує телефонний номер як основу для реєстрації, а підтвердження відбувається через SMS або голосовий дзвінок. Додатково підтримується двофакторна аутентифікація (2FA).

• Шифрування даних. Для звичайних чатів Telegram використовує клієнт-серверне шифрування на основі AES-256, RSA-2048 і протоколу обміну ключами Diffie-Hellman.

• End-to-end шифрування. Для «секретних чатів» застосовується End-to-end шифрування, що забезпечує доступ до повідомлень лише відправнику та отримувачу.

1.3.5 Опис механізмів протоколу MTProto, структури пакетів та характеристик системи Telegram

MTProto — це власний протокол Telegram, розроблений спеціально для забезпечення швидкої передачі даних із високим рівнем безпеки. Він складається з трьох основних компонентів:

– Авторизаційний ключ. Генерується під час першого з'єднання між клієнтом і сервером. Ключ використовується для шифрування всіх наступних сесій.

– Транспортний рівень. Забезпечує передачу даних через TCP, UDP або HTTP. MTProto підтримує адаптацію до нестабільних мереж.

– Шифрування повідомлень. Всі дані шифруються за допомогою алгоритму AES-256 у режимі IGE (Infinite Garble Extension).

Структура пакетів:

• Пакети MTProto включають:

* Заголовок із інформацією про тип даних, ідентифікатор сесії та час відправки.

* Зашифрований корисний вміст (текст повідомлення, медіафайли тощо).

• Сервери Telegram здійснюють маршалізацію пакетів і забезпечують швидку доставку даних.

Характеристики системи:

◇ Масштабованість. Telegram підтримує багатомільйонну базу користувачів завдяки розподіленій архітектурі серверів.

◇ Мобільність. Дані користувачів синхронізуються між пристроями в режимі реального часу.

◇ Гнучкість. Telegram дозволяє створювати боти, канали та групи для різних потреб.

1.3.6 Теоретичне обґрунтування можливих вразливостей протоколу MTProto

Хоча MTProto є унікальним і спеціально розробленим для Telegram, він піддавався критиці через деякі аспекти:

а) Критика унікальності протоколу. Деякі експерти вважають використання власного криптографічного протоколу менш безпечним, ніж застосування широко прийнятих стандартів, оскільки це ускладнює незалежний аудит.

б) Централізована інфраструктура. Telegram зберігає звичайні чати на своїх серверах, що робить їх уразливими до компрометації серверів.

в) Недостатній захист метаданих. Метадані, такі як час відправлення або IP-адреса, можуть бути доступні серверу Telegram.

Відомі дослідження:

– У 2015 році дослідники піддавали критиці MTProto за ймовірні недоліки в дизайні протоколу, хоча пізніше вони були спростовані командою Telegram.

– У 2020 році були знайдені вразливості, які дозволяли визначати, чи знаходяться двоє користувачів в одній групі, що пізніше було виправлено.

Таким чином, MTProto є ефективним протоколом для забезпечення швидкої та безпечної передачі даних, але потребує постійного вдосконалення для уникнення потенційних загроз.

1.3.7 Аналіз існуючої інформації про WhatsApp та його криптографічні механізми

WhatsApp — це один із найпопулярніших месенджерів у світі, що належить компанії Meta (раніше Facebook). Основна особливість WhatsApp — це використання **протоколу Signal** для забезпечення End-to-end шифрування, яке гарантує конфіденційність усіх повідомлень, дзвінків та файлів.

Основні криптографічні механізми WhatsApp:

1) End-to-end шифрування. Усі повідомлення шифруються на пристрої відправника та дешифруються лише на пристрої отримувача. Сервери WhatsApp не мають доступу до змісту повідомлень.

2) Аутентифікація користувачів. Верифікація здійснюється через телефонний номер із додатковим використанням SMS-коду для реєстрації.

3) Алгоритми шифрування. Signal Protocol базується на таких алгоритмах:

∇ AES-256 у режимі CBC для шифрування повідомлень.

∇ HMAC-SHA256 для перевірки цілісності даних.

∇ Протокол обміну ключами Double Ratchet для динамічного оновлення ключів шифрування після кожного повідомлення.

1.3.8 Опис механізмів протоколу Signal, структури пакетів та характеристик системи WhatsApp

Signal Protocol — це сучасний протокол шифрування, розроблений для забезпечення максимальної безпеки комунікацій. Він складається з кількох важливих компонентів:

1) Обмін ключами.

◇ Під час першого з'єднання між користувачами здійснюється обмін початковими ключами за допомогою алгоритму X3DH (Extended Triple Diffie-Hellman).

◇ Ключі шифрування автоматично оновлюються після кожного повідомлення через механізм Double Ratchet.

2) Шифрування повідомлень.

◇ Всі повідомлення шифруються на основі сесійних ключів, які регулярно оновлюються.

◇ Кожне повідомлення містить унікальний криптографічний ключ, що унеможливлює повторне використання одного й того ж ключа.

3) Транспортний рівень.

◇ Шифровані дані передаються через сервери WhatsApp для маршрутизації, але сервери не мають доступу до ключів дешифрування.

Структура пакетів:

а) Пакети WhatsApp включають:

* Заголовок із інформацією про відправника, одержувача та тип даних.

* Зашифрований вміст (текст повідомлення, медіафайли тощо).

б) Сервери WhatsApp використовуються лише для доставки пакетів і не зберігають змісту повідомлень.

Характеристики системи:

– Універсальність. WhatsApp підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами та створення групових чатів.

– Синхронізація. Хоча всі дані зашифровані, WhatsApp дозволяє резервне копіювання чату в хмарні сервіси (Google Drive, iCloud) із можливістю шифрування.

– Продуктивність. Завдяки оптимізованим серверам забезпечується висока швидкість доставки повідомлень навіть при низькій якості з'єднання.

1.3.9 Теоретичне обґрунтування можливих вразливостей протоколу Signal у WhatsApp

Хоча Signal Protocol вважається одним із найзахищеніших протоколів, у контексті WhatsApp можливі певні ризики:

1) Компрометація резервних копій. Якщо користувачі не активують шифрування резервних копій у хмарі, зміст повідомлень може стати доступним зловмисникам або провайдерам.

2) Уразливість метаданих. WhatsApp не шифрує метадані, такі як час відправлення, номер відправника й одержувача, що може бути використано для аналізу поведінки користувачів.

3) Доступ до ключів пристрою. Якщо зловмисник отримає фізичний

доступ до пристрою, можлива компрометація ключів шифрування.

4) Централізація серверів. Дані маршрутизуються через сервери WhatsApp, що теоретично створює можливість державного чи корпоративного тиску на компанію для доступу до метаданих.

Відомі дослідження:

◇ У 2019 році дослідники з Check Point виявили уразливість, яка дозволяла змінювати зміст повідомлень у групових чатах, але ця проблема була швидко виправлена.

◇ Інші дослідження акцентують увагу на проблемі збору метаданих, хоча Meta стверджує, що не використовує їх для таргетованої реклами.

Таким чином, WhatsApp забезпечує високий рівень захищеності завдяки Signal Protocol, але питання метаданих і резервного копіювання залишаються потенційними векторами атак.

1.3.10 Аналіз існуючої інформації про Viber та його криптографічні механізми

Viber — це популярний месенджер, розроблений компанією Rakuten, який забезпечує обмін повідомленнями, голосовими та відеодзвінками. Основна увага приділяється приватності та безпеці користувачів, що досягається за допомогою End-to-end шифрування для всіх типів комунікацій.

Основні криптографічні механізми Viber:

* End-to-end шифрування. Всі текстові повідомлення, дзвінки, медіафайли та інші типи даних автоматично шифруються, забезпечуючи доступ до змісту лише відправнику та отримувачу.

* Аутентифікація користувачів. Верифікація виконується через телефонний номер із використанням SMS-коду для реєстрації.

* Алгоритми шифрування. Viber використовує алгоритми AES-256 для шифрування даних і RSA-2048 для обміну ключами.

* Код автентичності повідомлень. Реалізовано механізм HMAC (Hash-

Based Message Authentication Code) для перевірки цілісності повідомлень.

1.3.11 Опис механізмів протоколу, структури пакетів та характеристик системи Viber

Пропрієтарний протокол безпеки **Viber Protocol** включає кілька важливих етапів:

1) Обмін ключами.

∇ При першій установці з'єднання між користувачами відбувається обмін асиметричними ключами RSA-2048.

∇ Сеансові ключі для шифрування даних генеруються за допомогою алгоритму Diffie-Hellman.

2) Шифрування даних.

∇ Повідомлення та дзвінки шифруються на основі сеансових ключів за допомогою AES-256.

∇ Кожне повідомлення має унікальний ключ, що запобігає компрометації історії повідомлень навіть у разі компрометації одного ключа.

3) Транспортний рівень.

∇ Дані передаються через сервери Viber лише для маршрутизації. Сервери не зберігають змісту повідомлень.

Структура пакетів:

– Заголовок із інформацією про ідентифікатори відправника та отримувача.

– Зашифрований вміст (текст повідомлення, голосові дані тощо).

– Хеш для перевірки цілісності.

Характеристики системи:

• Універсальність. Viber підтримує текстові повідомлення, дзвінки, групові чати, стікери, а також бізнес-аккаунти.

• Приватність. Повідомлення автоматично видаляються з серверів Viber після доставки.

• Доступність. Месенджер доступний на різних платформах,

включаючи iOS, Android, Windows та macOS.

1.3.12 Теоретичне обґрунтування можливих вразливостей протоколу Viber

Незважаючи на високий рівень безпеки, у системі Viber можливі певні вразливості:

∇ Централізація серверів. Хоча сервери Viber не зберігають змісту повідомлень, вони використовуються для маршрутизації, що може стати вектором для атак.

∇ Уразливість резервних копій. Якщо резервні копії повідомлень не шифруються у хмарному сховищі, можливий доступ до даних сторонніми особами.

∇ Недостатній захист метаданих. Інформація про відправника, одержувача та час відправлення може бути доступна серверу.

∇ Проблеми з фізичним доступом. Компрометація пристрою користувача може призвести до витоку ключів шифрування.

Відомі дослідження:

→ У 2016 році дослідники виявили уразливості, пов'язані з відновленням історії повідомлень через нешифровані резервні копії. Цю проблему було виправлено.

→ У 2017 році були зафіксовані атаки типу MitM у незахищених мережах Wi-Fi, які також були враховані та усунуті.

Таким чином, Viber забезпечує високий рівень захищеності завдяки використанню сучасних алгоритмів шифрування, проте централізація серверів та резервні копії можуть залишатися потенційними точками вразливості.

1.3.13 Порівняльний аналіз можливостей систем, їх криптографічних механізмів та рівня захищеності

Криптографічні механізми та рівень захищеності сучасних месенджерів є критично важливими для вибору користувачами найбільш безпечної платформи для комунікації. У наступній таблиці наведено ключові характеристики систем, їх переваги та недоліки для полегшення порівняння.

Таблиця 1.1 – Порівняльний аналіз характеристик систем обміну повідомленнями

Параметр	**Skype**	**Telegram**	**WhatsApp**	**Viber**
Протокол шифрування	Пропрієтарний, Signal для чатів	MTProto	Signal Protocol	Пропрієтарний
End-to-end шифрування	Лише для приватних чатів	Увімкнено за бажанням	Увімкнено за замовчуванням	Увімкнено за замовчуванням
Обмін ключами	RSA	Diffie-Hellman	X3DH	Diffie-Hellman
Аутентифікація	RSA, TLS	RSA, SHA-256	Curve25519, HMAC-SHA256	RSA, SHA-256
Основні алгоритми	AES-256, RSA	AES-256, SHA-256	AES-256, HMAC-SHA256, Curve25519	AES-256
Шифрування даних	AES-256	AES-256	AES-256	AES-256
Захист метаданих	Частковий	Обмежений	Немає	Немає
Використання серверів	Маршрутизація, зберігання	Маршрутизація	Маршрутизація	Маршрутизація
Доступність на платформах	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android

Таблиця 1.2 – Порівняльна таблиця основних переваг та недоліків месенджерів

Система	**Основні переваги**	**Основні недоліки**
Skype	- Інтеграція з Microsoft. - Підтримка голосових і відеодзвінків високої якості.	- Пропрієтарний протокол. - End-to-end шифрування обмежене лише приватними чатами.
Telegram	- Висока швидкість передачі даних. - Можливість великих групових чатів.	- End-to-end шифрування потрібно вмикати вручну. - Недостатній захист метаданих.
WhatsApp	- Використання Signal Protocol. - End-to-end шифрування за замовчуванням для всіх чатів.	- Збір і аналіз метаданих. - Уразливість резервних копій у хмарі.
Viber	- End-to-end шифрування за замовчуванням. - Повідомлення не зберігаються на серверах після доставки.	- Обмежений захист метаданих. - Залежність від центральних серверів.

Загальний висновок:

1) Найвищий рівень захищеності: WhatsApp завдяки впровадженню Signal Protocol та end-to-end шифруванню за замовчуванням.

2) Середній рівень захищеності: Telegram та Viber через залежність від централізованих серверів і обмежений захист метаданих.

3) Найменший рівень захищеності: Skype через пропрієтарний характер протоколу, часткове шифрування і залежність від серверів Microsoft.

1.3.14 Рекомендації користувачам щодо безпечного використання таких систем.

Ось рекомендації для користувачів щодо безпечного використання месенджерів Skype, Telegram, WhatsApp і Viber.

1) Загальні рекомендації для всіх месенджерів:

- Оновлюйте додатки. Завжди використовуйте останню версію

месенджера, щоб уникнути використання відомих вразливостей.

• Двохфакторна автентифікація. Увімкніть двохфакторний захист, якщо ця функція доступна, щоб ускладнити несанкціонований доступ.

• Уважність до підозрілих повідомлень. Не відкривайте підозрілі посилання або файли від невідомих контактів.

• Шифрування резервних копій. Якщо ви використовуєте резервні копії (наприклад, у хмарі), перевірте, чи вони захищені шифруванням.

• Конфіденційність облікового запису. Обмежте видимість свого профілю (наприклад, фото, статусу) для незнайомих осіб.

2) Skype:

• Використовуйте функцію «Приватні розмови» для чутливих даних, оскільки вона забезпечує end-to-end шифрування.

• Не зберігайте особисту інформацію у відкритих групових чатах, де доступ можуть мати сторонні.

• Використовуйте лише офіційний додаток Skype для входу в обліковий запис Microsoft.

3) Telegram:

• Увімкніть функцію «Секретні чати» для важливих повідомлень — це забезпечить end-to-end шифрування.

• У налаштуваннях конфіденційності приховайте номер телефону, якщо це не обов'язково.

• Регулярно перевіряйте активні сесії в налаштуваннях і завершуйте ті, які ви не впізнаєте.

4) WhatsApp:

• Перевіряйте безпеку ключів для контактів (функція в налаштуваннях), щоб уникнути атаки «людина посередині».

• Використовуйте шифрування резервних копій у Google Drive чи iCloud, увімкнувши відповідну функцію в налаштуваннях.

• Уникайте надання доступу додатку до конфіденційних даних або фото, якщо це не обов'язково.

5) Viber:

• Увімкніть функцію прихованих чатів для обміну чутливою інформацією.

• Перевіряйте відмітки про шифрування для кожного чату (значок замка).

• Не використовуйте публічні групи для обговорення конфіденційних тем.

6) Рекомендації для організацій та бізнесу:

• Використовуйте корпоративні версії месенджерів (наприклад, Microsoft Teams замість Skype) для підвищеного рівня безпеки.

• Обмежуйте використання месенджерів для передачі критичних корпоративних даних.

• Проводьте тренінги з кібербезпеки для співробітників, зосереджуючись на використанні комунікаційних платформ.

ВИСНОВКИ

Вибір месенджера залежить від ваших пріоритетів щодо конфіденційності, зручності та цілей спілкування. Якщо вам важливий високий рівень безпеки, найкращим вибором є **WhatsApp**. Він забезпечує end-to-end шифрування за замовчуванням для всіх чатів і використовує Signal Protocol — один із найнадійніших у світі. Це хороший вибір для звичайних користувачів, яким потрібна простота та надійність, але важливо враховувати, що платформа збирає метадані. Тому для ще більшої безпеки варто уникати створення незашифрованих резервних копій у хмарі.

Telegram також є хорошим варіантом, якщо ви готові вручну ввімкнути секретні чати для end-to-end шифрування. Цей месенджер пропонує високу швидкість передачі даних, підтримку великих групових чатів та зручність. Однак стандартні чати не мають end-to-end шифрування, а метадані захищені недостатньо, що може стати недоліком для користувачів, які цінують конфіденційність.

Viber є менш надійним у порівнянні з попередніми варіантами, хоча він забезпечує end-to-end шифрування за замовчуванням і видаляє повідомлення із серверів після доставки. Цей месенджер підходить для базового захисту, але має обмежений захист метаданих і використовує пропрієтарний протокол, що ставить під сумнів його прозорість і довіру до системи.

Що стосується **Skype**, то це хороший інструмент для бізнесу та відеодзвінків завдяки високій якості зв'язку та інтеграції з іншими продуктами Microsoft. Однак його безпека викликає сумніви через відсутність end-to-end шифрування для більшості чатів, закритий характер протоколу та слабкий захист метаданих.

Для максимальної безпеки обирайте WhatsApp або Telegram із секретними чатами. У будь-якому випадку, не забувайте про базові заходи: використовуйте двофакторну автентифікацію, створюйте складні паролі та шифруйте резервні копії, щоб забезпечити максимальний захист ваших даних.